



# Department of Homeland Security IAIP Directorate Daily Open Source Infrastructure Report for 24 September 2004

Current Nationwide  
Threat Level is



[For info click here](http://www.whitehouse.gov/homeland)  
[www.whitehouse.gov/homeland](http://www.whitehouse.gov/homeland)

## Daily Overview

- The Department of Energy has announced it intends to enter negotiations to make available a limited quantity of crude oil from the Strategic Petroleum Reserve, to help relieve physical shortages of crude oil supplies in the Gulf of Mexico following recent hurricanes. (See item [1](#))
- The U.S. Department of Agriculture, in partnership with the Food and Drug Administration and the Department of Homeland Security, on Thursday signed a cooperative agreement with the National Association of State Departments of Agriculture to further develop integrated federal-state response plans, in support of the National Response Plan, for food and agricultural emergencies. (See item [10](#))
- The Department of Homeland Security has launched Ready Business, an extension of its successful Ready campaign, that will help owners and managers of small to medium-sized businesses prepare their employees, operations and assets in the event of an emergency. (See item [18](#))
- The IDG News Service reports that computer code that takes advantage of a flaw in the way many Microsoft applications process JPEG images has been published on the Internet and could be a precursor to actual attacks on vulnerable PCs. (See item [23](#))

### **DHS/IAIP Update Fast Jump**

**Production Industries:** [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

**Service Industries:** [Banking and Finance](#); [Transportation](#); [Postal and Shipping](#)

**Sustenance and Health:** [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

**Federal and State:** [Government](#); [Emergency Services](#)

**IT and Cyber:** [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

**Other:** [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS/IAIP Web Information](#)

## **Energy Sector**

## **Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://esisac.com>]

1. *September 23, Department of Energy* — Department of Energy announces negotiations for loan of oil. The Department of Energy (DOE) announced on Thursday, September 23, that it intends to enter into negotiations to make available a limited quantity of crude oil from the Strategic Petroleum Reserve (SPR), to help relieve physical shortages of crude oil supplies in the Gulf of Mexico following recent hurricanes. The negotiations are for crude oil to be loaned under short-term contractual agreements from the SPR, and to be returned to the Reserve once supply conditions return to normal. Similar to the October, 2002 response to Hurricane Lili, these negotiations are being conducted following specific requests from refineries that have been affected by recent hurricanes. DOE's Energy Information Administration (EIA) statistics as of Friday, September 17, show a crude inventory drawdown of approximately 11 million barrels in the Gulf region over the past three weeks.  
Source: [http://www.energy.gov/engine/content.do?PUBLIC\\_ID=16691&BT\\_CODE=PR\\_PRESSRELEASES&TT\\_CODE=PRESSRELEASE](http://www.energy.gov/engine/content.do?PUBLIC_ID=16691&BT_CODE=PR_PRESSRELEASES&TT_CODE=PRESSRELEASE)

[[Return to top](#)]

## **Chemical Industry and Hazardous Materials Sector**

Nothing to report.

[[Return to top](#)]

## **Defense Industrial Base Sector**

2. *September 22, Federal Computer Week* — Army concerned about satellite use. Despite reasonable rates and excellent encryption, Army officials remain uncomfortable about the military's reliance on commercial satellites communications (satcom) to transmit voice, video and data during the war on terrorism. "We are very concerned about the amount of requirements put on commercial satellites," said Maj. General Dennis Moran, director of information operations, space and networks in the Army's Office of the Chief Information Officer. Military satellites provided 80 percent of communications and commercial satcom provided the remaining 20 percent for troops during the first Persian Gulf War in 1991. However, those numbers reversed during the current military conflicts in Iraq and Afghanistan. Moran said Army officials are awaiting the December 2005 launch of the first satellite in the \$1.3 billion Wideband Gapfiller Satellite program. The program involves "a high-capacity satellite system designed to support the warfighter with newer and far greater capabilities than those provided by current systems, yet is compatible with existing control systems and terminals," according to a contractor document.  
Source: <http://www.fcw.com/fcw/articles/2004/0920/web-satcom-09-23-04.asp>

[[Return to top](#)]

## **Banking and Finance Sector**

3. *September 23, Associated Press* — **EU, U.S. focus on charities to fund terror.** The United States and the European Union sought Thursday, September 23, to coordinate action against a growing problem of terrorist sympathizers using charities and cash couriers as covers to fund violence. U.S. Assistant Secretary of State E. Anthony Wayne said terrorists had been forced to use such methods by a successful international clampdown on funding through conventional banking. Wayne led a delegation that included officials from the U.S. state, justice and treasury departments in two days of talks with their EU counterparts on the fight against terrorist funding. **Pointing out that terrorists often operate on relatively small budgets, Wayne said customs officials in the United States and Europe needed to work closer together to deal with the problem of couriers conveying cash to terrorists.** He said nations around the world have different systems for monitoring charities. In the United States, tax authorities are working with counterterrorism officials to track funding channeled through charities. The United States is working with 32 other nations and regional groups through a Paris-based international watchdog, the Financial Action Task Force, to find agreed rules and standards on dealing with charities.

Source: [http://seattlepi.nwsourc.com/national/apeurope\\_story.asp?category=1103&slug=EU%20US%20Terror%20Funding](http://seattlepi.nwsourc.com/national/apeurope_story.asp?category=1103&slug=EU%20US%20Terror%20Funding)

4. *September 23, New Scientist* — **Most financial sites contain phishing flaws.** Nine out of 10 financial and commercial Websites contain flaws that could allow computer crooks to swindle users out of their cash, according to a new report. A study released by UK-based computer consultants Next Generation Security (NGS) on Thursday, September 23, reveals that **90% of the 100 financial companies audited by the company in the past year were vulnerable to an advanced phishing scam.** The majority of flaws discovered by NGS did not involve fake Websites as is usual with phishing attacks. Instead, **NGS most frequently found configuration errors that could be used to redirect sensitive information from a legitimate Website to a fraudulent one without the user knowing.** Known as a cross-site scripting attack, the trick uses a site's own server software to forward sensitive information, usually by embedding a link to another site in a complex hypertext link. A further 30% of sites analyzed by NGS were found to contain database vulnerabilities that could be used to access large amounts of personal information stored by a company. Study:

<http://www.ngssoftware.com/papers/NISR-WP-Phishing.pdf>

Source: <http://www.newscientist.com/news/news.jsp?id=ns99996439>

[\[Return to top\]](#)

## **Transportation Sector**

5. *September 23, Washington Post* — **Anti-terror measures delaying green cards.** The number of foreigners who became permanent U.S. immigrants dropped sharply in 2003 as anti-terrorism measures delayed the processing of applications, according to a new government report. The report, by the Department of Homeland Security, showed that 705,827 people became legal permanent residents in fiscal 2003, down from 1.06 million the year before. The Washington area recorded a 22 percent decline. A permanent-resident document, known as a "green card," allows an immigrant to live and work indefinitely in the United States and is the first step toward citizenship. **The decline does not mean that immigration is drying up. In fact, the number of newly arrived legal immigrants declined just seven percent. Most of**

those affected by the trend were foreigners already here — students, workers and others — who were hoping to become permanent residents. Only 347,416 got green cards in 2003, roughly half the number as in the previous year, because of the slowdown in processing. Although many of those immigrants were in the United States on temporary visas, the delays in getting permanent papers often caused hardship, immigrant advocates and attorneys said. Federal authorities defended their performance, saying they have had to deal with a host of new security measures after the September 11, 2001, terrorist attacks.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A43159-2004Sep 22.html>

6. *September 22, Reuters* — **US Air seeks deeper cost cuts from pilots.** Bankrupt airline US Airways has made a new proposal to its pilots that seeks nearly \$1.9 billion in savings through 2009, more than the \$1.5 billion originally proposed, according to a published report Wednesday, September 22. **The seventh-largest U.S. carrier asked the pilots union for a 19.5 percent pay cut, according to the Wall Street Journal. The company reached a tentative agreement on concessions with the union that represents its dispatchers. US Airways is seeking cuts in contributions to the pilots retirement plan, as well as increases in monthly flight hours and other productivity incentives.** If the pilots and other labor groups don't voluntarily agree to cost savings in the coming days or weeks, US Airways could ask U.S. Bankruptcy Court Judge Stephen Mitchell for permission to impose new terms on the workers, the Journal said. Meanwhile, the deal with the company's dispatchers covers about 150 of the airline's 28,000 employees. The deal is the first between the company and its unionized groups, which are key to the airline's efforts to cut costs and streamline its operations.

Source: [http://money.cnn.com/2004/09/22/news/fortune500/us\\_air.reut/index.htm?cnn=yes](http://money.cnn.com/2004/09/22/news/fortune500/us_air.reut/index.htm?cnn=yes)

[[Return to top](#)]

## **Postal and Shipping Sector**

Nothing to report.

[[Return to top](#)]

## **Agriculture Sector**

7. *September 23, Agence France Presse* — **Anthrax outbreak worsens. An anthrax outbreak which has killed close to 200 buffaloes, elephants, and a hippo in Botswana has spread to Namibia where it is posing a serious threat to livestock, officials said.** Game rangers have found the carcasses of 180 buffaloes, 10 elephants, and a hippo at Chobe National Park in northern Botswana since the outbreak on September 8. "We have received reports that the disease has crossed into Namibia. We are trying to establish how," wildlife acting district coordinator Obert Gwapela said. The outbreak has forced authorities to close about half of the park which is a major tourist attraction and is home to the Chobe river on the border between Namibia and Botswana. The permanent secretary in the Namibian ministry of environment and tourism, Malan Lindeque, told Agence France Presse that five elephants and four buffaloes had died but added that officials suspected the animals had contracted the disease in Botswana and died shortly after crossing the border to Namibia. "Our concern now is the livestock of the rural people. Our officials of veterinary services are busy vaccinating the livestock and are burning

all carcasses found to prevent the spread of anthrax in Namibia."

Source: [http://story.news.yahoo.com/news?tmpl=story&cid=1507&ncid=1507&e=2&u=/afp/20040923/hl\\_afp/botswana\\_namibia\\_health\\_040923\\_133722](http://story.news.yahoo.com/news?tmpl=story&cid=1507&ncid=1507&e=2&u=/afp/20040923/hl_afp/botswana_namibia_health_040923_133722)

8. *September 23, Nebraska Ag Connection* — **NDA accepting animal location information.** The Nebraska Department of Agriculture (NDA) is encouraging those who handle livestock, poultry, and other food animals to register the locations where their animals are kept under the State's new premises identification system. NDA has recently officially opened the premises identification portion of its Nebraska Animal Verification Enhancement (NAVE) system. A premises is a location where animals are kept, or will be kept, and can include a number of places, such as farms, ranches, auction markets, and county fairgrounds. The U.S. Department of Agriculture (USDA) has reviewed the premises part of the NAVE system and found it in compliance with national data standards.

Source: <http://www.nebraskaagconnection.com/story-state.cfm?Id=537&y r=2004>

9. *September 22, Mid-South Horse Review* — **New requirements for horse dealers.** The Tennessee Department of Agriculture on Wednesday, September 22, announced the implementation of new licensing requirements for horse dealers. Individuals who engage in the resale of horses are now required to be licensed by the department as a "livestock dealer" as a result of legislation passed by the General Assembly earlier this year. **"The significance and benefit of this legislation is that we now have the ability to trace transactions involving horses in the event of a disease outbreak or exposure,"** said Ron Wilson, State Veterinarian. Under state law, a livestock dealer is any person who buys, receives, or assembles livestock for resale either for their own account or on behalf of another person. Previously, state law defined livestock as cattle, swine, sheep, or goats. The new legislation now includes horses in the definition of livestock. **Under the Livestock Dealer Law, a dealer must secure an annual license from the Tennessee Department of Agriculture. Dealers are required to maintain records, especially the names and addresses of sellers and buyers of livestock, and make them available to the department upon request.** Wilson says that the new requirement is also an important tool in safeguarding the public and livestock industry from agri-security threats.

Source: <http://www.midsouthhorsereview.com/articles/2004/09/22/news/news10.txt>

[[Return to top](#)]

## **Food Sector**

10. *September 23, Food and Drug Administration* — **Agreement to make food supply more secure.** The U.S. Department of Agriculture (USDA), in partnership with the Food and Drug Administration (FDA) and the Department of Homeland Security (DHS), Thursday, September 23, signed a cooperative agreement with the National Association of State Departments of Agriculture (NASDA) to further develop integrated federal-state response plans, in support of the National Response Plan, for food and agricultural emergencies. This agreement advances one of the many homeland security directives set by President Bush to improve federal, state, and local cooperation through enhanced response and recovery procedures in the event of a disaster. USDA's Food Safety and Inspection Service (FSIS), FDA, and DHS's Information Analysis and Infrastructure Protection are funding the development of an integrated approach to prepare for and respond to emergencies affecting



national agriculture and food infrastructure. The state departments of agriculture will gain technical expertise from FSIS, FDA, and DHS officials through workgroups and tabletop exercises. Best practices and guidelines for federal and state food regulatory officials will be developed to address lessons learned from case studies and threat assessments.

Source: [http://www.fda.gov/bbs/topics/news/2004/usda\\_092304.html](http://www.fda.gov/bbs/topics/news/2004/usda_092304.html)

[\[Return to top\]](#)

## **Water Sector**

11. *September 23, Boston Globe* — **Pollutant discovered in treated waste water. Extremely high levels of perchlorate have been found in water flowing out of waste–water treatment plants in Billerica and Lowell, MA, but officials aren't sure how the chemical got there and whether it is linked to the presence of the pollutant in Tewksbury's drinking water.** The state announced last week that results from a round of samples taken a week earlier along the Concord River showed water leaving Billerica's waste–water treatment plant had a perchlorate level 158 times the limit recommended by state guidelines. Earlier in the month, test results showed the water flowing out of the Lowell Regional Wastewater Treatment Utility into the Merrimack River contained perchlorate levels about 20 times the recommended limit. "This is the first time that we're aware of, that perchlorate has been found in waste–water treatment plants" anywhere in the country, said Ed Kunce, deputy commissioner for the state Department of Environmental Protection. Kunce said he is conferring with environmental representatives from about 40 states, as the state investigates the cause and measures the effects of the chemical. A waste–water treatment plant takes in raw sewage that has been channeled through underground pipes, removes the solid wastes, and filters and disinfects the water so it can return in a purified form to the river. The cleaning process is critical because several communities draw their drinking water from the rivers.  
Source: [http://www.boston.com/news/local/articles/2004/09/23/pollutant\\_discovered\\_in\\_treated\\_waste\\_water/](http://www.boston.com/news/local/articles/2004/09/23/pollutant_discovered_in_treated_waste_water/)
12. *September 23, Fayetteville Observer (NC)* — **Acid reaches drain system. Some of the hydrochloric acid spilled at a Fayetteville, NC, chemical company Tuesday, September 21, leaked into the storm drain system downtown, officials said.** The company, Univar USA Inc., hired workers Wednesday, September 22, to clean the drainage pipes between the Worth Street spill site and Cross Creek, where storm water discharges. Univar, which distributes industrial chemicals, spilled 500 gallons of the acid on its grounds when a valve on a rail tanker broke. Jennings McArthur, senior engineer and technician for the city's storm water management system, said fewer than 20 gallons of acid leaked into the system.  
Source: <http://www.fayettevillenc.com/story.php?Template=news&Story=6579236>
13. *September 23, Washington Post* — **Early tests show germs in District's water.** Preliminary tests this month of the District of Columbia's water have registered some of the highest bacteria levels since summer 1996, when the city warned some people to boil tap water because of possible contamination, federal officials said Wednesday, September 22. In recent weeks, DC Water and Sewer Authority (WASA) has increased its disinfection treatment and flushing of distribution pipes to ease the problem, WASA officials said. **WASA officials said that they surmise that the addition this summer of a new chemical to curb high lead levels is**

**contributing to the peeling of bacteria film from pipe surfaces.** That is natural and was expected, said WASA chief engineer John Dunn, but may be happening at a faster rate than predicted. So far, 8.4 percent of the 143 tests the utility has analyzed have found positive readings of total coliform bacteria, common in soils, plants, and animals. The agency must take at least 210 tests but could take more by the end of the month. The Environmental Protection Agency considers water to have potentially unsafe levels of bacteria when more than five percent of the monthly tests are positive.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A43808-2004Sep 23.html>

[[Return to top](#)]

## **Public Health Sector**

14. *September 23, Associated Press* — **Vaccine could stem meningitis. Federal health advisers said Wednesday, September 23, that they were satisfied with the safety and effectiveness of a longer-lasting vaccine against bacterial meningitis.** But additional study will be needed to watch for any unexpected complications that could arise when the vaccine reaches a wider population, advisers to the Food and Drug Administration (FDA) said. The vaccine protects against the A, C, Y, and W-135 strains of bacteria that cause meningococcal diseases. The vaccine, being considered for people ages 11 to 55, still needs approval from the FDA. The agency often follows its advisers' recommendations but is not bound by them. More than 500,000 cases of meningococcal disease occur each year in the world, causing 135,000 deaths. Up to 15 percent of survivors have long-term problems, including mental disability, loss of hearing, and paralysis.

Source: <http://www.myrtlebeachonline.com/mld/myrtlebeachonline/news/politics/9733661.htm>

15. *September 22, National Institute of Allergy and Infectious Diseases* — **Potential new way to control drug-resistant bacteria.** Based on an improved understanding of bacteriophages — viruses that infect bacteria — scientists believe they have discovered a potential new way to control drug-resistant bacteria, an increasingly worrisome public health problem. The new research, funded by the National Institute of Allergy and Infectious Diseases (NIAID), found that bacteriophages contain genes that allow them to quickly change their proteins to bind to different cell receptors. **The researchers, who encountered this genetic property while working on an unrelated project, believe that this discovery could lead to the use of genetically engineered phages to treat bacterial infections that have become resistant to antibiotics.** "This research opens up numerous possibilities for developing drugs and vaccines that can control resistant bacteria, which are a growing public health concern," said David L. Klein, who oversees bacterial respiratory disease research at NIAID. **"The introduction of bacteriophages may also lead to a unique approach against biodefense-related pathogens."**

Source: [http://www.eurekalert.org/pub\\_releases/2004-09/nioa-sdp092204.php](http://www.eurekalert.org/pub_releases/2004-09/nioa-sdp092204.php)

16. *September 22, Chelmsford Independent (MA)* — **Towns to form medical reserve.** Westford, MA, Board of Health is the lead agency for the recently established Upper Merrimack Valley Medical Reserve Corps (MRC), a collaborative regional team that will serve more than a quarter of a million people in seven communities: Billerica, Chelmsford, Dracut, Lowell, Tewksbury, Tyngsboro, and Westford. Its volunteer ranks will include local doctors,

nurses, dentists, EMTs, pharmacists, respiratory therapists, social workers, counselors, and clergy members. These same seven communities make up the Upper Merrimack Valley Public Health Coalition, funded by the Massachusetts Department of Public Health. **The main purpose of the Medical Reserve Corps is to respond to large-scale disasters, whether it be a public health emergency — an influenza epidemic, outbreak of smallpox or anthrax — or a "mass casualty incident" like a fire, explosion, or terrorist act in which huge numbers of people are injured.** The nature of a large-scale disaster is that it is unexpected, it overwhelms existing resources, and produces a sudden influx of patients. The MRC provides "surge capacity" to supplement existing police, fire, and medical personnel, which are unequipped to handle hundreds or thousands of patients/victims in immediate crisis.

Source: <http://www2.townonline.com/chelmsford/localRegional/view.bg?articleid=89703>

[[Return to top](#)]

## **Government Sector**

17. *September 22, Government Accountability Office* — GAO-04-1075T: **Homeland Security: Observations on the National Strategies Related to Terrorism (Testimony).** The Government Accountability Office's (GAO) preliminary analysis of the national strategies related to terrorism identifies six departments—the Departments of Defense, Energy, Health and Human Services, Department of Homeland Security (DHS), Justice, and State—as having key roles in implementing the Homeland Security strategy. These six departments represent 94 percent of the proposed \$47 billion budget for homeland security in fiscal year 2005. In addition, these six departments have lead agency roles in implementing the Homeland Security strategy. For example, the DHS was designated as the lead agency for 37 of the 43 initiatives in that strategy. According to information received from agency officials, at least one of these six departments has demonstrated planning and/or implementation activities in each of the 43 initiatives. As key departments continue to implement the Homeland Security strategy, the development of performance goals and measures will help them assess their progress in implementing homeland security efforts.

Source: <http://www.gao.gov/new.items/d041075t.pdf>

[[Return to top](#)]

## **Emergency Services Sector**

18. *September 23, Department of Homeland Security* — **DHS and business organizations launch Ready Business.** The Department of Homeland Security (DHS), in partnership with the Advertising Council and a variety of business organizations, on Thursday, September 23, launched Ready Business. This extension of Homeland Security's successful Ready campaign, which has helped millions of individuals and families prepare for emergencies, focuses on business preparedness. **Ready Business will help owners and managers of small to medium-sized businesses prepare their employees, operations and assets in the event of an emergency.** DHS Secretary Tom Ridge said, "Ready Business was created to help encourage every business to develop an emergency plan, thereby making our nation and our economy more secure." An emergency preparedness plan can greatly improve the likelihood



that a company will survive and recover from all emergencies, natural disasters or terrorist attacks, but, too few businesses are taking the necessary steps to prepare. One of the key findings of the 9–11 Commission report was the need for the private sector to prepare for potential disasters. Ready Business, is designed to make emergency planning easier. For more information on Ready Business, see <http://www.dhs.gov/dhspublic/display?content=4034>  
Source: <http://www.dhs.gov/dhspublic/display?content=4035>

19. *September 23, Rock Hill Herald (SC)* — **New 911 system will contact residents in event of emergency.** Chester, SC, emergency 911 officials are prepared to use a new emergency notification system for weather–related problems, neighborhood water emergencies and even hostage situations. The Communicator, an emergency notification center at the E911/EMS office has as its centerpiece a computerized map of Chester county, said E911/EMS director Ginny Sloan. The system was purchased with a \$34,000 Homeland Security grant. **The automated system can illustrate individual homes or specific areas of a neighborhood. It then can be programmed to record a message on residents' phones if there is an emergency to which they need to be alerted. Messages can be recorded on the system to inform residents of emergencies including, for example, information of an Alzheimer's patient who has wandered from home, a chemical spill or a hostage situation. In the event of a hostage situation the call would go to each home except where the incident occurs, Sloan said.** If needed, the system will be used for weather–related problems such as tornado drills to inform schools, business and residents. The system recently was used to inform residents of the Lakewood subdivision, where a water tank exploded, that the water was not safe to drink, Sloan said.

Source: <http://www.heraldonline.com/local/story/3836579p-3438446c.html>

20. *September 23, Santa Cruz Sentinel (CA)* — **Teams face WMD threat during drill at Salz tannery.** A drill involving a possible chemical leak at Salz tannery in Santa Cruz, CA, on Wednesday, September 22, had the local bomb squad practicing how to disarm a biological weapon. **The nearly six–hour drill on weapons of mass destruction (WMD) involved the Santa Barbara county bomb squad, the Environmental Health Department and the county Hazardous Materials Interagency Team, as well as the Department of Forestry and Fire Protection.** "It's good for us to learn how to work together," said sheriff's Sgt. Amy Christey, one of the sheriff's six bomb technicians. The activity also prepared the agencies for the slight but not impossible chance they'll face a real–life dirty bomb situation one day. Under the drill's scenario, the Santa Cruz Fire Department was called around 9 a.m. to the historic leather factory that's been closed for three years. Firefighters arrived to find a bomb that, if exploded, would release hydrofluoric acid into the air. The chemical is attracted to calcium and, when it comes into contact with the skin, eats away at the tissue and muscle to get to the bone. By 12:30 p.m. the device had been deactivated and the hazardous materials crew had moved in to stop the chemical leak and clean up the remnants. Later, the bomb unit disposed of the explosives. The training exercise was deemed a success.

Source: <http://www.santacruzsentinel.com/archive/2004/September/23/local/stories/06local.htm>

[[Return to top](#)]

## **Information Technology and Telecommunications Sector**

21. *September 23, The Register (UK)* — **Firms ignore insider risk.** Company chiefs are aware of the threats of information security breaches posed by their employees, but are failing to safeguard their assets against insider attack. Keeping control of security will only get more difficult as organizations move toward increasingly decentralized business models through outsourcing and other external partnerships, Ernst & Young's 2004 Information Security Survey warns. **The Ernst & Young survey found that organizations remain focused on external threats such as viruses, while internal threats are consistently under-emphasized. More than 70 percent of the 1,233 organizations questioned by Ernst & Young failed to list training and raising employee awareness of information security issues as a top initiative.** Report: [http://www.ey.com/global/download.nsf/US/Global\\_Information\\_Security\\_Survey\\_-\\_2004/\\$file/2004\\_Global\\_Information\\_Security\\_Survey\\_2004.pdf](http://www.ey.com/global/download.nsf/US/Global_Information_Security_Survey_-_2004/$file/2004_Global_Information_Security_Survey_2004.pdf)  
Source: [http://www.theregister.co.uk/2004/09/23/insider\\_risk/](http://www.theregister.co.uk/2004/09/23/insider_risk/)
22. *September 23, SecurityTracker* — **redhat-config-nfs may set incorrect export permissions.** A vulnerability was reported in redhat-config-nfs versions prior to 1.0.13-6. The utility may set incorrect permissions on exported shares, potentially allowing unauthorized users to access the shares. A vendor fix is available; refer to SecurityTracker Alert for download details.  
Source: <http://www.securitytracker.com/alerts/2004/Sep/1011402.html>
23. *September 22, IDG News Service* — **Exploit posted for Microsoft JPEG flaw.** Computer code that takes advantage of a flaw in the way many Microsoft applications process JPEG images has been published on the Internet and could be a precursor to actual attacks on vulnerable PCs. The code was published late last week, only days after Microsoft revealed the "critical" vulnerability and made patches available to fix the problem. **Microsoft is urging all customers to immediately install the software updates it made available with Security Bulletin MS04-028:** <http://www.microsoft.com/technet/security/bulletin/MS04-028.msp>  
Source: [http://www.computerworld.com/securitytopics/security/story/0\\_10801.96088.00.html?f=x73](http://www.computerworld.com/securitytopics/security/story/0_10801.96088.00.html?f=x73)
24. *September 22, Reuters* — **Pentagon widens access to Website for overseas voters.** A Pentagon-run Website, <http://www.fvap.gov>, intended to make it easier for Americans overseas to vote by absentee ballot has been modified to broaden access to the site, the Defense Department said on Wednesday, September 22. The agency said the changes were made in response to concerns that some U.S. citizens living abroad and trying to access the Federal Voting Assistance Program's Website were blocked by security measures to deter hackers.  
Source: <http://www.reuters.com/newsArticle.jhtml?type=internetNews&storyID=6310532>
25. *September 22, Computerworld* — **Virus knocks out Colorado DMV systems.** A computer virus has knocked out computer systems at the Colorado Division of Motor Vehicle offices in Colorado Springs since Friday, September 17. As a result, no documents, identification cards or driver's licenses are expected to be issued until at least Monday, September 27, according to DMV spokesperson Diane Reimer. Reimer said she doesn't believe any personal data has been lost, and she said the virus didn't affect other government agencies.  
Source: [http://www.computerworld.com/securitytopics/security/story/0\\_10801.96095.00.html?f=x73](http://www.computerworld.com/securitytopics/security/story/0_10801.96095.00.html?f=x73)

26. *September 22, SecurityTracker* — **Symantec Gateway Security lets remote users modify the configuration.** Several vulnerabilities were reported in Symantec Gateway Security. A remote user can determine the services active on the target device and can also determine and modify the device configuration settings. Symantec Enterprise Firewall is also affected. The vendor has released a fixed version (firmware build 622) for Symantec Gateway Security 320, 360 and 360R and a fixed firmware version (v1.63) for Symantec Enterprise Firewall Models 100, 200 and 200R: <http://www.symantec.com/downloads/>  
Source: <http://www.securitytracker.com/alerts/2004/Sep/1011388.html>
27. *September 22, iDEFENSE* — **Sophos Anti-Virus fails to detect malicious code in files named with reserved DOS device names.** A vulnerability was reported in Sophos Anti-Virus as packaged with Sophos Small Business Suite. A remote user can create malicious code that will evade the anti-virus detection capabilities. The vendor is releasing a fixed version (3.86).  
Source: <http://www.odefense.com/application/poi/display?id=143&type=vulnerabilities>
28. *September 22, SecurityTracker* — **Apache Satisfy directive error may let remote users access restricted resources.** A vulnerability was reported in Apache <httpd> version 2.0.51 in which a remote user may be able to gain access to restricted resources. A fix is available in Apache <httpd> 2.0.52-dev: <http://httpd.apache.org/>  
Source: <http://www.securitytracker.com/alerts/2004/Sep/1011385.html>
29. *September 22, SecurityTracker* — **CA Unicenter Management Portal lets remote users determine valid account names.** A vulnerability was reported in CA's Unicenter Management Portal. A remote user can determine valid account names on the target application. A vendor workaround is available in the SecurityTracker Alert.  
Source: <http://www.securitytracker.com/alerts/2004/Sep/1011381.html>

### Internet Alert Dashboard

<p align="center"><b>DHS/US-CERT Watch Synopsis</b></p> <p><b>Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.</b></p> <p><b>US-CERT Operations Center Synopsis:</b> Microsoft released a new security bulletin detailing critical vulnerabilities in the way it handles JPEG graphics. More information can be found here:  <a href="http://www.microsoft.com/technet/security/bulletin/ms04-028.msp">http://www.microsoft.com/technet/security/bulletin/ms04-028.msp</a>.</p>	
<p align="center"><b>Current Port Attacks</b></p>	
<p><b>Top 10 Target Ports</b></p>	<p>445 (microsoft-ds), 135 (epmap), 1434 (ms-sql-m), 137 (netbios-ns), 9898 (dabber), 5554 (sasser-ftp), 1023 (Reserved), 4000 (Connect-BackBackdoor), 1026 (nterm), 1027 (icq)</p> <p>Source: <a href="http://isc.incidents.org/top10.html">http://isc.incidents.org/top10.html</a>; Internet Storm Center</p>

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Website: [www.us-cert.gov](http://www.us-cert.gov).

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[\[Return to top\]](#)

## **Commercial Facilities/Real Estate, Monument & Icons Sector**

Nothing to report.

[\[Return to top\]](#)

## **General Sector**

Nothing to report.

[\[Return to top\]](#)

### **DHS/IAIP Products & Contact Information**

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP Web page (<http://www.nipc.gov>), one can quickly access any of the following DHS/IAIP products:

[DHS/IAIP Alerts](#) – Advisories and Information Bulletins: DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact.

[DHS/IAIP Daily Open Source Infrastructure Reports](#) – The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open-source published information concerning significant critical infrastructure issues.

[DHS/IAIP Daily Reports Archive](#) – Access past DHS/IAIP Daily Open Source Infrastructure Reports.

### **DHS/IAIP Daily Open Source Infrastructure Report Contact Information**

Content and Suggestions:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS/IAIP Daily Report Team at (703) 883-3644.

Subscription and Distribution Information:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS/IAIP Daily Report Team at (703) 883-3644 for more information.

### **Contact DHS/IAIP**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure

Coordinating Center at [nicc@dhs.gov](mailto:nicc@dhs.gov) or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

**DHS/IAIP Disclaimer**

The DHS/IAIP Daily Open Source Infrastructure Report is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.